

Corporate IT Security Policy



Confidential

August 2001

Version 1.0

Table of contents

1.	Introduction	1
2.	General Definitions.....	1
3.	Security Organization	2
3.1.	Information security coordination.....	2
3.2.	Allocation of information security responsibilities.....	2
3.3.	Authorization process for information processing facilities	2
3.4.	Security requirements from third party contracts	3
3.5.	Outsourcing	3
4.	Asset Classification and Control	3
4.1.	Asset management	3
4.2.	Information classification	4
4.3.	Information labeling	4
5.	Personnel Security	4
5.1.	Personnel attitude	4
5.2.	Security awareness	5
5.3.	Reporting of security incidents.....	5
6.	Physical and Environmental Security	6
6.1.	Physical Security.....	6
6.2.	Equipment Security.....	6
6.3.	Clear desk.....	7
7.	System Development and Maintenance.....	7
7.1.	System Operations and Administration	7
7.2.	System Testing.....	7
7.3.	Controls against malicious software.....	7
7.4.	Information Backup and Housekeeping	8
7.5.	Network controls.....	8
7.6.	Media handling and security	8
7.7.	Data Exchange	9
8.	System Access Control	9
8.1.	Access control policy	9
8.2.	Access management.....	9
8.3.	Network access control	10
8.4.	Logging and monitoring	10
8.5.	Mobile computing.....	10
9.	Communications and Operations Management.....	10
9.1.	Commercial software implementation	10
9.2.	Cryptography	10
9.3.	System operations and management.....	11
9.4.	Change control procedures.....	11
10.	Business Continuity Planning	11
10.1.	Business continuity management process	11
10.2.	Preventing the impact of cyber crimes	11
11.	Compliance	12
11.1.	Legal requirements	12
11.2.	Safeguarding of organizational records	12
11.3.	Privacy requirements.....	12
12.	Security Policy	12
12.1.	Applicability	12
12.2.	Sanctions.....	12

Revision history

Revision number	Date	Author	Comments
0.1	07/27/01	Daniel Durocher	Pre-release
0.5	07/31/01	Daniel Durocher	Overall revisions; added Definitions and ASP concepts
0.51	08/13/01	Daniel Durocher	Minor revision after comments; issued to Security Council for revision
0.52	08/16/01	Daniel Durocher	Creation of an index
0.53	08/29/01	Daniel Durocher	Added definition of Contractor; minor change to cover page and inclusion of comments by Roger Bricker, Greg Martin and Les Wilson; upgrade to the index.
1.0	08/31/01	Daniel Durocher	First official corporate release

1. Introduction

Security policies are designed to provide “enforceable, measurable, action statements and ways of working” regarding attitude to risk and other hard to define parameters. The IT Security Policy is the mother of all security related policies by virtue of the principles that it puts forward.

2. General Definitions

Computer Incident Response Team A multi-functional task force who’s main objective is to curb cyber-attacks.

Contractor Someone who is retained to perform a certain act or service. Unlike an employee, an independent contractor pays for all expenses, social security, and income taxes and receives no employee benefits.

Digital Signature The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine:

- whether the transformation was created using the key that corresponds to the signer’s key; and
- whether the message has been altered since the transformation was made.

Distinguished Name The unique name assigned to a node in a Directory Information Tree (DIT).

Director of Corporate Security A person who’s responsibilities encompass the broad spectrum of the organization security: physical security, IT Security and Network Security. This role has an overall technical function as well as responsibilities for the strategic focus of the organization’s global security needs.

Directory A directory system that conforms to the RFC 1777 of the Internet Engineering Task Force (IETF).

Employee An employee is any person employed in or by a department who has been authorized to access electronic networks.

Information Security Officer A person who’s responsibilities is to ensure that information security policies and procedures are established and implemented to protect the information assets of an organization, participate in the creation and review of the policies and procedures, recommend security strategies, and keep information security systems current.

Management A group of senior individuals who are devoted to the strategic aspects aimed at building a successful organization in all key sectors. They usually include individuals who share a vice-presidency or similar strategic functions.

Threats and Risks Assessment An analysis aimed at establishing all the threats facing the organization and evaluating the exposure (the risk).

User Requirement Specification A specification that documents the purposes for which a system is required. This document must be issued by the requester of the system.

3. Security Organization

3.1. Information security coordination

The senior management of Jamcracker will lead by example by ensuring that Information Security is given a high priority in all current and future business activities. This attitude is required by our use and by our adoption of this business model. Therefore, the high priority given to security must encompass the whole Jamcracker ecosystem where we shall lead by example.

As part of this commitment to IT security, Jamcracker is committed to providing regular and relevant Information Security awareness communications to all staff by using a variety of means: e-mail, all hands meeting, the intranet and others, as required.

3.2. Allocation of information security responsibilities

All of the organization's system must be managed by a team of qualified system administrators who will be responsible for overseeing the day-to-day operations and security of the systems. System administrators must be fully trained to administer the specific platform for which they are responsible. Additionally, they must be knowledgeable of the security threats they are facing and must have proper training in defending against them and in performing adequate security configurations.

All proposed system enhancements must be business driven and supported by an approved business case. Ownership and responsibility for any such enhancements will rest with the business owner of the system.

3.3. Authorization process for information processing facilities

All purchases of new system software, hardware or new components for existing systems must be made in accordance with IT Security and other organization policies. Such requests to purchase must be based upon a User Requirement Specification document and take into account longer-term organizational business needs. This specification documentation lists the purpose for which a system is required and must be considered essential to the process.

The office automation suite links the different business systems at Jamcracker. In consequence, only office automation packages that are compatible to the approved computer operating system and office automation platform may be used. Other licensed software installation, irrespective of its distribution model, must be approved by IT Security and restricted to stand-alone workstation where appropriate tests can take place before being deployed to networked workstations.

All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Security aspects pertaining to the installation must also be discussed and planned ahead of the proposed installation date. As such, all systems must be comprehensively tested and fully accepted by users before being transferred to the live environment, once security configurations have been formally tested and approved by Corporate Security.

3.4. Security requirements from third party contracts

All parties involved in e-business systems and delivery channels including contractors, *Application Service Providers (ASP)* and any other type of Service Providers, must be able to meet the requirements and objectives of Information Security at Jamcracker. Appropriate Service Level Agreements (SLAs) must be thorough and must be completed prior to starting such a service delivery.

Third party contractors must be able to demonstrate their security awareness and knowledge or agree to attend security awareness seminars or training when required by Jamcracker. Jamcracker must formally provide a summary of the IT Security policy to third party contractors prior to any supply of service.

When signoff is required for work accomplished by contractors, only formally authorized personnel may accept and sign for work done by third parties.

3.5. Outsourcing

Every company selected to outsource portions or all of Jamcracker business process must be able to demonstrate that it complies with the IT Security policy requirements. They must also provide a Service Level Agreement that documents the performance expected and the remediation and escalation procedures in the event of non-compliance.

Confidentiality must be ensured at all times and a non-disclosure agreement must be established between Jamcracker and its outsourcer prior to the start of any work. Breaches of confidentiality must be reported to the *Director of Corporate Security* as soon as detected.

4. Asset Classification and Control

4.1. Asset management

Every computer asset in the organization must be assigned an owner who will be responsible for it. Every computer must be accounted for in a hardware inventory that will list, at a minimum, the type, make, model, specifications, cost, location, owner and asset number. This inventory must be searchable with at least the two following criteria to insure a proper audit: asset number and owner.

Hardware and software documentation must be kept up-to-date and readily available to the support and operation personnel. Documentation

includes: the user's guide, the operation manual and any technical documentation supplied by the vendor.

All new and updated systems that are developed by the organization must be fully supported by an up-to-date documentation. New or updated systems must NOT be ported to the production environment unless supporting documentation is available and has been validated.

Additionally, Jamcracker must create and maintain a database of all information assets. An information asset is a definable piece of information, stored in any matter, which has a value to the organization.

4.2. Information classification

All information (data and documents) in the organization must be assigned an owner who will be responsible for it. Moreover, all this information must be classified according to the parameters defined in the **Data Classification Guidelines**.

All information, data or document classified as Secret must be stored in a separate secure area and must NOT be mixed with information, data or documents of lesser sensitivity classification. Data encryption techniques must be considered.

4.3. Information labeling

Clear and appropriate, as per the data classification, labeling must be applied to all information, data and documents so that all users are aware of the ownership and the classification of the information. For example, a document's security classification level and ownership should be indicated in the header and footer on each page of the document.

5. Personnel Security

5.1. Personnel attitude

Risks to Jamcracker's systems and information must be minimized. The first measure toward accomplishing this goal is to foster and keep a greater personnel awareness and rewarding staff vigilance about positive security actions aimed at increasing our overall security posture.

All employees must comply with the Information Security Policies that exist at Jamcracker. Any information security incident that is the result of non-compliance with the policies will result in immediate disciplinary action up to and including termination.

All personnel must have previous employment and other references carefully checked.

In order to preserve the confidentiality of our operation, only authorized personnel, trained for this function, may speak to the media about matters relating to Jamcracker. Communication with customers must also be carried out by personnel that has been authorized and trained for this function, who will recognize the nature of the information that they are

allowed to release. The former applies to telephone inquiries, formal or informal meeting and any kind of communication.

5.2. Security awareness

Information Security awareness tools must be provided to all Jamcracker employees in order to enhance awareness and educate them regarding the range of threats and the appropriate counter-measures. Such tools may include formal training, seminars, brochures, demonstration or information published on an intranet, as approved by the *Corporate Security department*.

As appropriate to the context, an adequate summary of the IT Security policy must be made available to temporary employees as well as third-party contractors.

The top management of Jamcracker is committed to this policy as described in section 3.1 of the present document.

As part of this effort, Jamcracker is committed to provide formal training to all users of new systems in order to ensure that they are both proficient with their use and that they do not compromise information security. Moreover, information security training is mandatory for all users. When personnel move to other positions across the organization, their security training needs must be re-assessed and new training, as required, must be given in priority.

Jamcracker must designate and train a user with an *Information Security Officer* (ISO) role. Periodic training must be given in priority to this person to ensure that education and training in the latest threats and Information Security techniques is adequate and up to date.

Technical personnel must receive training in Information Security topics as part of their overall job training, which consists of configuration adjustments and overall maintenance operations.

5.3. Reporting of security incidents

Jamcracker will establish and train on the latest threat and exploits a Computer Incident Response Team (CIRT) who will be responsible to identify, evaluate, contain and eradicate the cause of security incidents. This team will report to the Director of Corporate Security.

All suspected Information Security incidents must be reported promptly to the *Director of Corporate Security* who will have the responsibility to decide whether they need to be further investigated or reported to outside authorities. Employees may not attempt to respond to a security incident as Jamcracker risks losing evidence.

Any information security breach must be reported immediately to the Corporate Security department to speed up the identification of the damages done and facilitate the gathering of evidence. The Director of Corporate Security will be responsible to determine the appropriate course

of action to repair the breach of security and will report on a regular basis to upper management.

6. Physical and Environmental Security

6.1. Physical Security

The sites chosen to locate computers and to store data must be located in areas that are protected from physical intrusions, theft, fire, flood and other hazards. Physical access to computer premises must be protected from unauthorized entry using systems or technologies that can identify, authenticate and monitor all access attempts. All employees must be aware of the need to challenge strangers on the premises, especially those who do NOT wear a recognized badge.

Any location where data is stored (ex: vault for backup tapes) must also provide access control and adequate protection to prevent against loss or damage to data.

Physical access to high security areas is to be controlled with strong authentication technologies. Personnel with access to such areas must be provided with appropriate information on the security risks associated with their access.

6.2. Equipment Security

Computer equipment must be located in a secure facility or proper measures must be enforced to insure their protection from theft, loss and damage. Only authorized personnel are allowed to take equipment belonging to Jamcracker off the premises: they are responsible for its security at all times.

Equipment is always to be safeguarded with appropriate access control methods when left unattended. To protect information from unauthorized disclosure, all users of workstations, PC or laptop must ensure that their screen are blank when they are not being used. This may be accomplished by the use of a screen saver that will engage on request of automatically after a specified time.

Users of portable computers must be made aware of the information security issues related to their use and must implement the recommended safeguards to minimize the risks. All such equipment must be insured by a corporate insurance policy.

Deliberate or accidental damage to computer equipment owned by Jamcracker must be reported to the Corporate Security department as soon as they are noticed and the appropriate reports must be filed. Any movement or disposal of equipment must be strictly controlled by authorized personnel who have made sure that the security risks have been mitigated.

Network cabling must be installed and maintained by qualified technicians to ensure the integrity of the cabling and the wall jacks. Any unused network cable or jack must be sealed-off and their status must be recorded.

Employees issued with mobile phones that belong to the organization are responsible for using them in a manner consistent with the confidentiality level of the matter being discussed. Theft, damage or loss of mobile phone must be reported to the Corporate Security department as soon as they are noticed and the appropriate reports must be filed.

6.3. Clear desk

Jamcracker expects all employees to clear their desks at the end of each workday to ensure that sensitive documents are not exposed to unauthorized persons outside of normal working hours. Furthermore, any PC, server or workstation monitor must be blanked when left unattended (see section 6.2). A means of restricting the use of any unattended computer (either logical or physical) must be implemented and maintained active at all times.

7. System Development and Maintenance

Software developed by or for Jamcracker must always follow a strict and formalized development process and managed accordingly. Source code integrity must be maintained by using a combination of access controls, and tight privilege management controls enforced by robust procedures.

7.1. System Operations and Administration

System Operation schedule must be formally planned, authorized and documented to avoid system contention and poor data accuracy of the overall environment. Furthermore, Jamcracker management must ensure that proper segregation of duties is enforced in all areas dealing with system development, system operations and system administration.

7.2. System Testing

New systems must be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience that meets or exceeds the requirements and specifications before migrating to the production environment. Additionally, these tests must demonstrate that the new system will not induce any security threat when under load, through buffer overflows and other such parameters.

Formal change control procedures are mandatory for all modifications to systems. All changes to programs must be authorized and tested before being applied to the production environment (see section 9.4).

7.3. Controls against malicious software

The use of removable media such as diskettes, CD-ROM or Zip® disks is not allowed for importing data except when formally authorized. Their use could destroy valid system files in Jamcracker's environment and carry the risk of introducing computer viruses and worms. For these reasons, employees are not authorized to load screen savers onto any computers owned by Jamcracker unless they have a formal approval to do so.

Incoming e-mail must be considered a threat and must be treated as such. The opening of e-mail with file attachments is not allowed unless the attachment has already been scanned for viruses and other malicious code (worms, Trojan horses and other).

When sending e-mail, the file attachments are only allowed after these attachments have been scanned for viruses and malicious code. Moreover, the classification of the data file must be carefully considered before it is being transmitted via e-mail.

Every piece of information downloaded from the Internet must be scanned with the corporate anti-virus solution prior to be opened, used or executed. Unlicensed information and software may not be used on computers owned by Jamcracker or used to carry work commissioned by Jamcracker.

An anti-virus policy must be implemented to protect every PC on the organization. Signature files must be updated and distributed automatically on a regular basis, not to exceed one week, and formal procedures to respond to a virus incident must be developed, tested and assigned exclusively to a *Computer Incident Response Team* (see section 5.3 for more information on CIRT).

A definite set of procedures to handle hoax virus must also be implemented since hoax can draw away attention from the threat of real viruses.

7.4. Information Backup and Housekeeping

Sample applications and files must systematically be removed from production servers prior to their migration to this environment, to prevent misuse by unauthorized users. In addition, temporary files on user's PC must be deleted regularly to prevent potential misuse.

Backup of the organization's data file must be considered a top priority and data restore must be tested on a regular basis to ensure accuracy and a fair recovery time when failure occurs. Management is responsible to make sure that the frequency and the method of such backup operations and the methods used for recovery meet the business needs.

7.5. Network controls

The network must be designed and configured to deliver high performance and reliability to meet the business needs while providing a high degree of security through access controls and adequate privilege management.

7.6. Media handling and security

Any person required to use removable media such as diskettes must be explicitly authorized to do so. Removable media must be handled in a very cautious way as not to compromise the confidentiality of the organization's data. It is thus a requirement to consider the classification of the data that is copied onto removable media and handle it accordingly. Data encryption must be considered and used when available.

7.7. Data Exchange

Internal, confidential or secret data and information may only be transferred across networks or copied to external media when the confidentiality and integrity can be assured by means of encryption and digital signature.

The same type of information may only be sent by fax when more secure methods are not possible. The owner and the recipient of the information must both formally agree on this type of transmission beforehand.

8. System Access Control

A full set of access control standards must be formally sanctioned by Jamcracker's management in order to prevent unauthorized access on every system in use across the whole organization. Controls must be set so that access to sensitive and confidential data and information on projects owned or managed by Jamcracker is restricted to authorized employees only. Data must be protected against unauthorized or accidental tampering and may only be deleted with the proper authority.

8.1. Access control policy

A full set of access control standards must be developed by balancing the need to access data for business purposes against controlling access to the information assets. These standards must be built on the foundation provided by a formal data classification which applies to all information assets (see section 4.2).

Access to all systems must be authorized by the owner of the system and it, along with its associated access controls (or privileges), must be recorded in an Access Control List (ACL) that must be kept in a highly confidential manner. Access to information and document must be carefully controlled as to allow for authorized access only.

In order to reduce the probability of internal incidents, the access control standards and data classification must be maintained on a regular basis and a periodic review must be carried out at intervals.

Individuals responsible to configure the Internet access must make sure that Jamcracker's environment is protected against malicious activities according to the best practices of the industry. In that regard, the Human Resources department must take action to ensure that all resources having Internet access are aware of, and will comply with, an acceptable usage guideline for the Internet in addition to this Information Security policy.

8.2. Access management

User IDs must be assigned only to resources that have been approved explicitly by the Human Resources department who is responsible for maintaining a resource database. Upon notification of staff termination, the *HR manager* must make a recommendation on whether or not this access must be considered a threat and on the suitability to maintain the staff's access to the network resources.

Passwords are the primary mean of controlling access to systems. Therefore, password selection must be made in accordance with the ***Guidelines for Secure Password Selection*** published and maintained by Jamcracker.

8.3. Network access control

Access to network resources must be efficiently controlled to prevent their unauthorized use. Access to all computing and information systems and peripherals must be denied unless explicitly authorized. Care must be exercised when allowing user-IDs as not to reveal the extent of their privilege (ex: administrator, rootpriv, etc).

Remote access to Jamcracker's network and resources will be granted exclusively through strong identification and authentication procedures and will use encryption techniques to insure confidentiality and protect against eavesdropping.

8.4. Logging and monitoring

Errors and inconsistencies that occur during processing must be recorded in error logs. Error logs must be properly reviewed by qualified personnel to detect any suspect activity that may signal a security incident.

Access attempts must be logged and monitored to identify potential misuse of the system and unauthorized access.

8.5. Mobile computing

Mobile computers, including laptop computers, cellular phone, personal diary assistants, alpha and two-way pagers and others, must be secured and their access must be restricted by means of their internal capabilities, at a minimum (see section 6.3). The user must regularly backup the information stored on mobile computers to corporate servers.

9. Communications and Operations Management

9.1. Commercial software implementation

The implementation of new or upgraded software must be carefully planned and managed. Procedural and technical controls must be implemented to mitigate the risks associated with the added threats of such project.

9.2. Cryptography

Digital signatures must be applied to the exchange of confidential information to insure authentication and integrity. Strong Encryption techniques must be applied to protect the confidentiality of any document with a classification of private, confidential or secret.

Every Jamcracker employee may only use approved cryptography technology that is adopted as a corporate standard.

9.3. System operations and management

Jamcracker's system must be configured, operated and administered using documented procedures that comply with the best practices. These practices must be proven effective in protecting the information security.

During the testing phase of a project, the use of live data will only be allowed if appropriate controls for the security of data are in place.

9.4. Change control procedures

Change control procedures must always be applied to software development and documentation belonging to Jamcracker and its clients so that accurate decisions can be made and that software bugs can be eradicated. In addition, formal change control procedures must be applied to software updates and enhancements and formal authorization must be sought before a modification is made. Every change must be thoroughly tested before it is transferred in the production environment.

Vendor patches issued to resolve bugs must be acquired from a reputable source and their integrity must be verified. Patches may only be applied to production environment after they have been thoroughly tested and approved by management.

Operating system patches and any necessary upgrades must be carefully planned and have all their associated risk identified. Fallback procedures must be planned and tested before patches are being applied to the production environment.

10. Business Continuity Planning

Management of Jamcracker is required to initiate and develop a Business Continuity Plan (BCP), which covers all essential and critical business activities. To this end, management must undertake a formal *Threat and Risk Assessment* (TRA) in order to determine the requirements for the BCP.

All personal must be made aware of the Business Continuity Plan and training must be provided in order to raise awareness and set the expectations should the plan be activated. To ensure proper understanding, the BCP will be tested periodically, once implemented.

The BCP plan will be updated and re-tested periodically, in close relation with the evolving business context.

10.1. Business continuity management process

Owners of the enterprise information system used throughout Jamcracker must make sure that a *Disaster Recovery Plan* (DRP) has been developed, tested and implemented for their system. When an information system is outsourced, a DRP will be required as part of the Service Level Agreement (SLA) negotiated with the outsourcer.

10.2. Preventing the impact of cyber crimes

Jamcracker will prepare, maintain and test regularly a plan to address cyber-attacks. The purpose of this plan must be to ensure that damages

caused by such attacks may be reduced to an absolute minimum and that the enterprise can resume operations with only minimal delays.

11. Compliance

11.1. Legal requirements

Information from the Internet or other sources may not be used without the prior consent of its author. Care must be taken to protect intellectual property and privacy. As such, customer information must be considered confidential and appropriate controls must be enforced.

11.2. Safeguarding of organizational records

Jamcracker must perform the archiving of documents with due consideration to legal, regulatory and business issues. This activity must be carried only if a *Retention Policy* can be referred to.

11.3. Privacy requirements

Employee data is confidential and will not be released to another employee or external resource. Employee data may only be released to persons and/or organizations that have been formally authorized and with in accordance with procedures set forth in section 5.1.

12. Security Policy

12.1. Applicability

All full-time employees, part-time employees, third party contractor making use of Jamcracker's IT infrastructure and anyone using it must abide by the requirements of the IT Security Policy.

Outsourcers and other partners must be provided with an adequate summary of this policy and they must comply with its entirety.

12.2. Sanctions

The inappropriate use of Jamcracker's systems, accounts and resources, the unauthorized use of another person's computer account, and providing false or misleading information for the purpose of obtaining access to computer systems or modifying data, are prohibited and will be subject to the sanctions listed below. Any other violations of any provision of this policy may also result in:

- **limitation** on a user's access to some or all systems,
- the initiation of **legal action** by Jamcracker, including, but not limited to, criminal prosecution under appropriate state and federal laws,
- the requirement of the violator to provide **restitution** for any improper use of service, and
- **disciplinary actions**, up to and including termination.

References

Web Links

A Beginner's Guide to Network Security	www.cisco.com
A Multi-Dimensional Approach to Internet Security	http://www.avolio.com/MultiDimensional.html
Dynamic Host Configuration Protocol	http://www.normos.org/rfc2131.txt
Georgia Tech Information Security	http://www.oit.gatech.edu/security/security/usage/draftpolicy.html
Improving Network and Computer Security at the University of California, Berkeley	http://ist-socrates.berkeley.edu:2001/security/itatf_swg_report.html#AI
InfoSec in the Real World: A Pragmatic Approach to Implementing a Corporate Security Policy	http://securityportal.com/articles/infosec_realworld20010716.printerfriendly.html
ISO 17799: Compliance and positioning	http://www.securityauditor.net/iso17799/
IT Security Cookbook	http://www.boran.com/security/zindex.html
New York State Office for Technology – Technical Policies	http://www.oft.state.ny.us/policy/99-2.htm
NIST Security Policy Documents	http://csrc.ncsl.nist.gov/secplcy/
RUSecure Information Security Policies	www.eon-commerce.com/rusecure
SANS Model Security Policy	http://www.sans.org/newlook/resources/policies/policies.htm
Security Best Practices for Application Service Providers (ASPs)	http://www.jawzinc.com/main.asp

Books and Publications

Garfinkel, S. & Spafford, G., Web Security & Commerce, O'Reilly Nutshell, 1997, 506 p.

Internal documents

Internet Usage Policy, JC-11-0022
Guidelines for Secure Password Selection (2001)
Guidelines for Encryption of Data (2001)
Guidelines for Data Classification (2001)

Others

International Standard ISO/IEC 17799, Information technology – Code of practice for information security management, First edition, Geneva

Index

A

Access control
 ACL, 9
 Authentication, 6, 7, 8, 9, 10
ASP, 3, 13
Audit, 1, 3, 9, 10

B

Business continuity planning, 11

C

Cabling, 7
 Jacks, 7
CIRT, 1, 5, 8
Computer
 Media, 7, 8

D

Data classification, 4, 8, 9, 10
Disaster recovery plan, 11
Documentation, 2, 3, 4, 11
Download
 Files, 8
 Legal requirements, 12
 MP3 and others, 12

E

E-mail, 2, 8
Encryption
 Digital signature, 9, 10

G

Guidelines, 4, 9, 10, 13

I

Installation
 Hardware, 3
 Scheduling, 3
 Software, 2
Intellectual property, 12

L

Labeling, 4
Laptop, 6, 10
Logs, 10
 Error logs, 10
 Monitoring, 10

M

Mobile computing
 Cellular phones, 10

O

Outsourcing, 3, 12
 Contracts, 3

P

Privacy, 12
 Employee data, 12
Privileges
 Administrator, 2, 10

R

References, 13
Roles
 Director of Corporate Security,
 1, 3, 5
 HR Manager, 9
 Information Security Officer, 1,
 5

S

Security
 Challenge response, 6
 Equipment, 6
 Incident, 1, 4, 5, 8, 9, 10, 11
 Mobile phones, 7, 10
 Password, 10, 13
 Physical security, 1, 6, 7
 Reporting, 5, 6, 7, 13
 Screen saver, 6, 7
 User ID, 2, 9, 12
Service Level Agreement, 3, 11
Source code, 7

T

Training, 2, 3, 4, 5, 11
 Awareness, 2, 3, 4, 5, 11

V

Virus, 7, 8
 Hoax, 8
 Signature files, 8

